WHAT IS CLAIMED IS:

1. A method of biometric verification comprising the steps of:
establishing parameters of a software application;
generating a biometric template from a set of user's initialization biometric data;
generating an access software application based on said software application parameters and said biometric template; and
securing said access software application using tamper-resistant software techniques;
thereby allowing said access software application to be stored locally, yet be secure.

2. The method of claim 1 wherein said step of generating a biometric template comprises the steps of:
querying a user to input multiple initialization copies of a biometric feature;
reading said multiple initialization copies; and
calculating a biometric template based on said multiple initialization copies.

3. The method of claim 2 wherein said step of calculating comprises the step of calculating a biometric template using pattern recognition techniques.

4. The method of claim 1 wherein said step of securing comprises the step of:
storing said biometric template in a format different than that required at the input to said access software application.

5. The method of claim 1, wherein said access software application is operable to perform the steps of:
challenging said user to input an access copy of said biometric feature;
comparing said input access copy of said biometric feature to said biometric template, and responding to said input access copy being a match by performing the steps of:
generating a secure password from said biometric template; and
updating said biometric template;
otherwise, generating an incorrect password.

6. The method of claim 5, wherein said step of generating a secure password comprises the step of generating a high-quality cryptographic key.

7. The method of claim 5, wherein said step of generating a secure password comprises the step of generating the private key of a public/private key pair.

8. The method of claim 5 wherein said access software application is operable to generate different secure passwords corresponding to different verification thresholds.

9. The method of claim 1 wherein said step of securing comprises the steps of:
encoding said access software application using data flow encoding.

10. The method of claim 5 wherein said step of securing said access software application comprises the step of:
obscuring the data in said biometric template.

11. The method of claim 5 wherein said step of securing comprises the step of:
transforming the data flow in said access software application to dissociate the observable operation of the transformed said access software application from the intent of the original software code.

12. The method of claim 5 wherein said step of securing comprises the step of:
encoding the data flow in said access software application into a domain which does not have a corresponding semantic structure, to increase the tamper-resistance and obscurity of said access software application.

13. The method of claim 1 wherein said step of securing comprises the steps of:
encoding said access software application using control flow encoding.

14. The method of claim 5 wherein said step of securing said access software application comprises the step of:
obscuring said step of comparing in said access software application.

15. The method of claim 5 wherein said step of securing comprises the step of:
transforming the control flow in said access software application dissociate the observable operation of the access software application from the intent of the original software code.

16. The method of claim 5 wherein said step of securing comprises the step of:
dispersing subsequences of instructions within said access software application into a plurality of locations;
merging multiple dispersed subsequences into single blocks of code;

selecting said subsequences of instructions from merged blocks of code for either functionally effective or decoy execution, as needed, to separate the observable operation of resulting code from the intent of the original software during execution.

17. The method of claim 5 wherein said step of securing comprises the step of:
adding fake-robust control transfers to said access software application, to increase the tamper-resistance of said access software application.

18. The method of claim 1 wherein said step of securing comprises the steps of:
encoding said access software application using mass data encoding.

19. The method of claim 5 wherein said step of securing comprises the step of:
encoding said biometric template, using mass-data encoding techniques.

20. The method of claim 5 wherein said step of securing comprises the step of:
responding to a request to store a data value at a virtual address by:
mapping said virtual address onto a randomly selected actual address; and
storing said data value in a memory location indexed by said actual address.

21. The method of claim 1 wherein said step of securing comprises the steps of:
encoding said access software application using white box encoding.

22. The method of claim 5 wherein said step of securing comprises the step of:
representing one or more algorithmic steps or components as tables, thereby permitting encodings to be completely arbitrary nonlinear bijections.

23. The method of claim 5 wherein said step of securing comprises the step of:
identifying functions and transforms substantive to the targeted software program;
generating new functions and transforms which alter the processing activity visible to the attacker; and
replacing those identified functions and transforms with the new functions and transforms in the software program.

24. The method of claim 1, in which the level of obscurity is sufficient to make attacks on stored biometric and template prohibitively expensive for attackers.

25. The method of claim 1, in which said step of securing is performed after said step of establishing parameters of a software application, and said step of securing comprises the step of:

securing said access software application by applying tamper-resistant software techniques to said parameters.

26. An electronic device operable comprising:

means for establishing parameters of a software application;

means for generating a biometric template from a set of user's initialization biometric data;

means for generating an access software application based on said software application parameters and said biometric template; and

means for securing said access software application using tamper-resistant software techniques.

27. A computer readable memory medium for storing software code executable to perform the method of any one of claims 1 - 25.

28. A carrier signal incorporating software code executable to perform the method of any one of claims 1 - 25.

29. A data structure comprising the output data of any one of claims 1 - 25.